Phishing
Phishing is the fraudulent practice of sending emails that appear to be from reputable companies to trick individuals into revealing sensitive information like account details, passwords, and credit card numbers. Some common methods for identifying phishing include:
- Suspicious or Slightly Changed Sender Email Address
- Destination Email Address/Recipient is Incorrect
- Urgent or Time-sensitive Response Requested
- Embedded Links or Attachments
- Asking for Confidential Information
- Asking for Payment Information
- Spelling and Grammar Errors

Spear Phishing
This type of phishing is targeted and personalized to a specific individual, group, or organization. Cybercriminals send emails to specific and well-researched targets while acting as a trusted sender. The goal is to either infect devices with malware or convince victims to hand over personal information or money.

Whaling
Whaling is a highly targeted phishing attack that targets end users that include high profile individuals like politicians, celebrities, and corporate executives to steal sensitive information. This is designed to encourage victims into authorizing high-value wire transfers to the attacker.
Phishing emails can be created to mimic any company, non-profit, or person. They're designed to create urgency and drive a quick reaction from you. Understanding this, if you received an email like the sample below, what would you reaction be?

Some tips to help determine email validity:
1. Ask yourself if it makes sense that you should be getting an urgent shipping communication.
2. Look at the sender's email address. The domain (@paradanta.com) doesn't appear to be legitimate nor match something from UPS.
3. Without clicking anything, hover your mouse over a link to see where you are really being directed. Notice that the company name in the link is incorrect. UPS doesn't have “servicing” in its name.

This is a simplistic example of a phishing email. It's important to understand that hackers are getting increasingly better at building convincing emails. Therefore, you need to take the time to review emails with a critical eye.

Being educated in identifying phishing techniques is key to avoiding hacks. Contact PCS to learn about Phishing Training options designed to help keep you informed and safe.

PCS Locations:
NEW JERSEY - MOORESTOWN 856.596.4446
NEW JERSEY - VINELAND 856.596.4446
NEW JERSEY - NORTHFIELD 856.596.4446
NEW JERSEY - RED BANK 732.456.8828
NEW YORK 732.456.8828
MASSACHUSETTS 617.546.5446
PENNSYLVANIA 215.426.1049
CALIFORNIA 951.234.3432
www.helpmepcs.com